REMARKS

Applicant amends claims 16, 17, 19-23, 26-28, 32-34, and 36. The amendments are supported, e.g., by paragraph [0019] of the published U.S. Patent Publication no. 2007/0127394. The independent claims have been amended to be similar to the subject matter previously presented in claims 29 and 37. Consequently, claims 29-31 and 37 are canceled without prejudice or disclaimer. Claims 16-28, 32-34, and 36 are presently pending.

35 U.S.C. §103(a) Rejections

The Examiner rejected claims 16-18, 21-25, 28, 29, 31, 32, 34, and 37 under 103(a) being unpatentable over Rune (U.S. Patent Publication no. 2004/0167988) in view of O'Neill (U.S. Patent no. 7,339,903). Applicant respectfully disagrees. The currently pending independent claims are claims 16, 21, 22, and 32. These claims have been amended to recite certain similar subject matter.

Claim 16 is representative and is reproduced below (this claim is shown in a form after the present amendment).

> A method comprising:
>
> checking a destination address of a received packet;
>
> comparing the destination address of the packet with at least one predetermined multicast and/or broadcast address;
>
> preventing the transmission of the packet to a first device in response to the addresses matching; and
>
> forwarding the packet to at least the first device in response to the addresses not matching.

The Examiner states the following:

> However Rune does not explicitly teach comparing the destination address of the packet with at least one predetermined multicast and/or broadcast address and in response to the addresses matching/in response to the addresses not matching. However, O'Neill teaches if a multicast packet is received, it is determined whether or not the address of the multicast packet is in its visitor list; if not, the packet is forwarded; if the address matches an address list, the packet is dropped **[see column 17 lines 42-58]**. It would have been obvious for a person having ordinary skill in the art to compare the destination address of the packet with at least one predetermined multicast and/or broadcast address and preventing the packet in response to the addresses matching; and forwarding in response to the addresses not matching. This is desirable because it prevents packets from being floods to all the sub-networks needlessly (see Rune paragraph 0210).

Outstanding Office Action, page 4. However, the Applicant's claims relate to a ***destination address*** of a packet: "checking a ***destination address*** of a received packet", "comparing the ***destination address*** of the packet with at least one predetermined multicast and/or broadcast address;" "preventing the transmission of the packet to a first device in response to the addresses matching;" and "forwarding the packet to at least the first device in response to the addresses not matching." By contrast, O'Neill recites the following (emphasis added):

> FIG. 8 is a flow diagram illustrating an exemplary method 232' that may be used to effect multicast forwarding operations at an access router (which may be or include a foreign agent). As indicated by trigger block 805, if a multicast packet is received from multicast transport, the method 232' proceeds to decision block 810. At decision block 810, it is determined whether or not the **source (sender) address** of the multicast packet is a persistent address in its visitor list. If not, the packet is forwarded to receivers registered with the multicast group as indicated by block 812 before the method 232' is left via RETURN node 870. (See, e.g., communications 1410, 1510 and 1610 of FIGS. 14, 15 and 16, respectively.) If, on the other hand, the **source address** matches a persistent address in its visitor list, the packet is dropped as indicated by block 815, before the method 232' is left via RETURN

> node 870. ***(This is because local multicast forwarded will have already been performed.)***

O'Neill, col. 17, lines 42-58. Note the sentence at the end of this paragraph: "This is because local multicast forwarded will have already been performed." This is further explained here:

> (5) The foreign agent (FA) checks its visitor list to see if the sender's address in incoming multicast packets from the core network is a host home address (HoA) in its visitors list. If this is the case, then the FA drops the multicast packet because local receivers will already have been served by these packets before they were tunneled to the home agent (HA) and is the equivalent to the processing when packets are sent to and received from an RP or with any unidirectional multicast tree delivery system.

O'Neill, col. 10, lines 44-53. That is, the sender's address is checked in O'Neill because if the sender's address is the host home address, the packet has already been sent via other pathways.

Applicant cannot find any location O'Neill where a destination address of a packet is checked and the packet forwarded to a device or the transmission of the packet prevented to the device based on the destination address of the packet.

Because the Examiner admits that "Rune does not explicitly teach comparing the destination address of the packet with at least one predetermined multicast and/or broadcast address and in response to the addresses matching/in response to the addresses not matching" (outstanding Office Action, page 4) and Applicant has shown that O'Neill does not disclose or imply this subject matter, the combination of Rune and O'Neill cannot disclose this subject matter. Therefore, claim 1 is patentable over the combination of Rune and O'Neill.

Because claim 1 is patentable, the other independent claims 16, 21, 22, and 32 are also patentable for at least the reasons given above with respect to claim 1. Because these independent claims are patentable, their dependent claims are also patentable.

Regarding Rune, what Rune states regarding broadcast types is the following (emphasis added)

> [0123] FIGS. 10-15 illustrate the coverage areas of the different broadcast types. The NAPSA broadcast type, as the name implies, is used to broadcast packets to a single NAPSA. This is illustrated in FIG. 10 (which is similar to FIG. 8), where each isolated gray area 1000-1008 represents a different NAPSA broadcast area. **A NAPSA broadcast packet is not allowed to leave its broadcast area.** Thus, NAPSA broadcast packets are not forwarded to the LAN and are not allowed to cross a NAPSA border.
>
> [0124] The scatternet broadcast type, as the name implies, is used to broadcast packets within the scatternet. This arrangement is illustrated in FIG. 11, where each contiguous gray area 1100-1106 represents different broadcast areas for a scatternet broadcast packet. **Such broadcast packets are not forwarded to the LAN.** When more than one AD exists in a scatternet, the scatternet broadcast packets carrying higher layer protocol packets, i.e. packets from protocol layers above the NAL, e.g. IP, are not allowed to cross an AD border. These packets are consequently limited to a part of the scatternet belonging to the same AD. Scatternet broadcast packets that are not carrying packets from higher layer protocols, such as NAL control packets, however, are allowed to cross AD borders and may therefore still be broadcast in the whole scatternet. A NAL control packet does not encapsulate data from a higher protocol layer and is only used to transfer signaling and control information between NAL entities in different Bluetooth nodes. This arrangement is illustrated in FIG. 12, where each contiguous gray area 1200 and 1202 represents the broadcast area of an NAL control packet.
>
> [0125] The AD broadcast type covers the LAN and any attached scatternets that are associated with the same AD as the LAN. These broadcast packets are forwarded by NAPs from/to the LAN to/from the scatternet, but the NAPSA borders in the scatternet are respected. This arrangement is illustrated in FIG. 13, where each contiguous gray area 1300-1304 represents the broadcast area of an AD broadcast packet. An AD broadcast packet is used to reach all the nodes in the AD (including the nodes on the LAN). All broadcast packets that are forwarded from the LAN to the scatternet are sent using the AD broadcast type.
>
> [0126] The scatternet-AD broadcast type is a special broadcast type used only for route requests. This broadcast type is, as the name implies, a combination of the scatternet broadcast type and the AD broadcast type. The scatternet-AD broadcast packets are distributed through the entire scatternet without respecting the NAPSA borders, as well as the entire AD via the NAPs.

> However, the NAPSA borders are respected after a scatternet-AD broadcast packet re-enters the scatternet via a NAP.

Thus, in Rune, the NAPSA broadcast packets are not forward to a scatternet, and the scatternet broadcast packets are not forwarded to the LAN. However, these packets are not forwarded based on their ***broadcast type***, which is defined by an indicator in a NAL (network adaptive layer) header (emphasis added):

> [0122] In addition to the routing protocol discussed above, the NAL also has a broadcast mechanism. (Note that broadcasting on the LAN is inherent in the shared medium and no "broadcast" mechanism is needed.) In accordance with embodiments of the invention, the NAL includes four different types of broadcasts: NAPSA broadcast, scatternet broadcast, AD broadcast, and scatternet-AD broadcast. The differences between broadcast types lie in the scope of the distribution and how the NAPs and other nodes at the NAPSA borders treat the different broadcast packets. **Note that the broadcast type is defined by an indicator in the NAL header.** In that sense, these different broadcast types can only exist in the scatternet. On the other hand, an Ethernet broadcast packet (originated on the LAN) that is forwarded from the LAN to the scatternet becomes an AD broadcast packet when it is forwarded into the scatternet. The broadcast type may be indicated in the NAL header, for example, with a two-bit indicator, as indicated in Table 2.

Thus, the broadcast type is defined in Rune by an indicator in the NAL header.

It is clear that filtering of broadcast packets in Rune is performed without examination of destination addresses for packets (emphasis added):

> [0196] The second main component of the invention is the packet filtering mechanism. As already mentioned, a NAP does not indiscriminately forward packets. Instead, it uses the packet filtering mechanisms (see FIG. 9) to reduce the number of unnecessarily forwarded packets. For example, forwarding is unnecessary when both the source and the destination node are located on the same side of the NAP. Furthermore, NAL broadcast packets of the NAPSA broadcast type and the scatternet broadcast type are always blocked by the packet filtering mechanisms. **Only those packets that pass the packet filtering mechanisms are forwarded to the scatternet.** The generated useless traffic is a waste of resources, especially so in the scatternet where radio resources and processing resources are scarce. Furthermore, this could lead to the scatternet being flooded by traffic from the LAN with its shared medium and much higher capacity. Therefore, a packet

> filtering mechanism is needed in order to limit the forwarding of unnecessary traffic. The packet filtering is based on the destination address and the NAL packet type. Filtering may also be based on higher layer protocols.
>
> [0197] The NAL packet type filtering in the NAP is performed in the packet type filtering function 912, which is present only on the scatternet side of the NAP. **The NAL packet type filtering**, in some embodiments of the invention, **is very simple: all *NAPSA broadcast type and scatternet broadcast type packets* are passed by the packet type filtering function 912 to the NAP-IPH, while *all other packet types* are passed to the address filtering function 914.**

Thus, packets having the NAPSA broadcast and scatternet broadcast ***types*** are filtered, and **all other packet *types*** are passed to an address filtering function, for forwarding to the correct address. See also, e.g., paragraphs [0222], [0224], [0237] of Rune.

As is noted in paragraphs [0125] and [0197] from Rune above, packets having the AD broadcast type are forwarded, as are packets having the scatternet-AD broadcast type (see paragraphs [0126] and [0197]).

Regarding multicast addresses, these appear to be related to route entries. See, e.g., the following:

> [0173] When (and if) the NAP-B of a NAP receives an encapsulated non-ARP-route-request (via the NAP-PFL), the NAP processes the non-ARP-route-request just like any node would process a received non-ARP-route-request. Thus, the NAP forwards the non-ARP-route-request into the scatternet, unless it already has a route to the destination node, or unless the NAP itself is the destination node. In the latter case, the NAP can immediately return an encapsulated non-ARP-route-reply. Then the next hop node in the route entry for the source node is indicated as "another NAP." This indication may be just a general indication, or it may be a specific indication that includes a NAP **multicast address** or the specific source MAC address of the Ethernet packet that carried the received encapsulated ARP-route-request. The choice between general indication, NAP multicast address or source MAC address depends on whether broadcast packets, multicast packets or unicast packets are used to carry a corresponding encapsulated ARP-route-reply.

See also paragraphs [0156], [0186], and [0187] of Rune. There are additional references to "multicast" in Rune, but none of these references relate to the subject matter of "comparing

the destination address of the packet with at least one predetermined multicast and/or broadcast address" and "preventing the transmission of the packet to a first device in response to the addresses matching" as recited in amended claim 16.

Applicant respectfully submit that this is further evidence the combination of Rune and O'Neill does not disclose at least the subject matter of "comparing the destination address of the packet with at least one predetermined multicast and/or broadcast address" and "preventing the transmission of the packet to a first device in response to the addresses matching" as recited in amended claim 16. Claims 21, 22, and 32 are also patentable for at least the reasons given above with respect to claim 16.

The dependent claims are also patentable over the combination of Rune and O'Neill for at least the reasons given above. It is noted that Applicant is not acquiescing to the combination of Rune and O'Neill; however, this combination need not be accessed at this time.

Additional 35 U.S.C. §103(a) Rejections

The Examiner rejected other dependent claims. For instance, the Examiner stated the following:

> 6. Claims 19,20,26,27,30 and 33 rejected under 35 U.S.C. 103(a) as being unpatentable over Rune as applied to claims 16-18, 21-25, 28,29,31, 32,34 and 37 above and further in view of Vasisht (US 2004/0133689).

Outstanding Office Action, page 15. The Examiner also stated the following:

7. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rune as applied to claims 16,18,21,22,25,28,29,31,32,34 and 35 above, and further in view of Tung (US 2006/0136562 A1) (herein after Tung).

Outstanding Office Action, page 18.

It is believed these two sets of rejections should use both Rune and O'Neill in addition to Vasisht and Tung.

Regardless, because independent claims 16, 22, and 32 are patentable, dependent claims 19, 20, 26, 27, and 33 are patentable for at least the reasons given above. Because independent claim 22 is patentable, its dependent claim 36 is patentable for at least the reasons given above.

Conclusion

Based on the foregoing arguments, it should be apparent that the pending claims are thus allowable over the reference(s) cited by the Examiner, and the Examiner is respectfully requested to reconsider and remove the rejections. The Examiner is invited to call the undersigned attorney for any issues.

Respectfully submitted:

2/28/11

Robert J. Mauri
Reg. No.: 41,180

Date

Customer No.: 10,948

HARRINGTON & SMITH, Attorneys at Law, LLC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400
Facsimile: (203)944-0245
email: rmauri@hspatent.com

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450 or is being transmitted electronically to the United States Patent and Trademark Office.

2.28.2011

Name of Person Making Deposit

Date